C.1 BACKGROUND

This effort provides the Department of Defense (DoD) and its interagency partners with research, development, test and evaluation, operations, maintenance, and training capabilities and related professional services that will meet dynamic capability development requirements.

C.1.1 PURPOSE

The purpose of this TO is to provide DoD and its interagency partners with research, development, test and evaluation, operations, maintenance, and training capabilities, cyber capability and tools development, advanced concepts support, data analytics, and related professional services. This initiative will rapidly provide capabilities and enhancement services through collaboration with Government and industry partners, and will assist in developing and strengthening cyberspace operations capabilities for operational forces.

C.1.2 AGENCY MISSION

The Office of the Deputy Assistant Secretary of Defense Office of Command, Control, And Communication (C3), Cyber, and Business Systems (C3CB), interacting with Department of Defense (DoD) and Intelligence Community mission partners analyzes requirements and discovers cutting edge technology in organizations (government, commercial, academic, and non-profit sectors). The agency also supports research, programmatic deliverables, justifications and recommendations for new technologies. These roles include support to the following:

a) Leading the development and implementation of Department-wide communications, command and control, and cyberspace architecture, technical framework, standards, and strategic approaches;
b) Performing Overarching Integrated Product Team responsibilities for selected Major Defense Acquisition Programs and Major Automated Information System programs;
c) Leading or supporting Analysis of Alternatives and studies as directed for selected capabilities;
d) Performing acquisition-related enterprise wide portfolio management and net-centric systems engineering across space, air, ground, maritime, and cyberspace domains;
e) Guiding and facilitating the communications, command and control, and cyberspace capabilities development through the Joint Capabilities Integration and Development System; Planning, Programming, Budgeting and Execution System; and Defense Acquisition Systems processes for all designated information technology and National Security Systems (NSS) programs; and
f) Providing technical direction and integration efforts across DoD components and synchronize critical DoD communications, command and control, and cyberspace capabilities.

C.2 SCOPE

The scope of this requirement provides capabilities and enhancement services through collaboration with Government and industry partners, supporting the developing and strengthening of cyber operations capabilities for operational forces.

Specifically, this requirement provides the following:

- Provide Program Management: This includes the management and oversight of all activities performed by contractor personnel to satisfy the requirements identified in this Statement of Work (SOW).
- Cyber Capability Development Support: The Contractor shall provide professional technical services to enhance cyberspace capabilities that implement cyberspace objectives. The Contractor shall further develop and enhance rapid prototypes in direct support to cyber operations performed by the operational users. The Contractor shall provide access and exploitation development, reverse engineering, vulnerability research, modeling & simulation, and application development for software, analytics, and systems.
- O&M Integration Support: The Contractor shall provide O&M support to include supporting the integration of operational technologies, providing engineering and hardware, software, and system administration. The contractor shall support information assurance best practices and formal accreditation processes.

C.3 CURRENT ENVIRONMENT

Potential state and non-state adversaries conduct malicious cyber activities against U.S. interests globally and in a manner intended to test the limits of what the United States and the international community will tolerate. Potential adversaries have invested significantly in cyber as it provides them with a viable, plausibly deniable capability to target the U.S. homeland and damage U.S. interests.

As cyber capabilities become more readily available over time, the DoD assesses that state and non-state actors will continue to seek and develop cyber capabilities to use against U.S. interests. The global proliferation of malicious code or software ("malware") increases the risk to U.S. networks and data.

The DoD's own networks and systems are vulnerable to intrusions and attacks. In addition to DoD's own networks, a cyberattack on the critical infrastructure and key resources on which DoD relies for its operations could impact the U.S. military's ability to operate in a contingency. DoD has made gains in identifying cyber vulnerabilities of its own critical assets through its Mission Assurance Program – for many key assets, DoD has identified its physical network infrastructure on which key physical assets depend – but more must be done to secure DoD's cyber infrastructure. In addition to destructive and disruptive attacks, cyber actors steal operational information and intellectual property from a range of U.S. government and commercial entities that impact the Defense Department.

C.4 OBJECTIVE

Specific objectives of this TO include:

- Vulnerability, security, data analytics support, and market research within DoD designated technologies and concepts;

- Creation, integration, operation, and maintenance of cyber development and experimentation environments, and conducting cyber experimentation for advanced capability and analytic support concepts;
- Development, delivery, and maintenance of cyber operations infrastructures, networks, platforms, capabilities, tools, and systems;
- Development and execution of quality control processes to include informal and formal Test and Evaluation (T&E) and documentation;
- Development and implementation of training and exercise environments, systems, documentation, and scenarios for DoD designated end users;
- Operational support for fielded capabilities in support of ongoing priority efforts.

C.5 TASKS

C.5.1 TASK 1 –PROJECT MANAGEMENT

The contractor shall provide project management support under this effort. This includes the management and oversight of all activities performed by contractor personnel to satisfy the requirements identified in this Statement of Work (SOW). The contractor shall identify a Project Manager (PM) by name who shall provide management, direction, administration, quality assurance, and leadership of the execution of this TO.

C.5.1.1 SUBTASK 1 –PROJECT KICK-OFF MEETING

The contractor shall schedule, coordinate, and host a Project Kick-Off Meeting at the location approved by the Government (Section F, Deliverable 02). The meeting will provide an introduction between the contractor personnel and Government personnel who will be involved with the TO. The meeting will provide the opportunity to discuss technical, management, and security issues, and travel authorization and reporting procedures. At a minimum, the attendees shall include Key Personnel, other contractor personnel, representatives from the directorates, other relevant Government personnel, and the FEDSIM COR.

At least three days prior to the Kick-Off Meeting, the contractor shall provide a Kick-Off Meeting Agenda (Section F, Deliverable 01) for review and approval by the FEDSIM COR and the Technical Point of Contact (TPOC) prior to finalizing. The agenda shall include, at a minimum, the following topics/deliverables:

a. Points of contact (POCs) for all parties
b. Draft Project Management Plan (PMP) (Section F, Deliverable 07) and discussion including schedule, tasks, etc.
c. Personnel discussion (i.e., roles and responsibilities and lines of communication between contractor and Government)
d. Staffing Plan and status
e. Security discussion and requirements (i.e., building access, badges, Common Access Cards (CACs))
f. Invoicing considerations
g. Transition discussion
h. Final Baseline Quality Control Plan (QCP) (Section F, Deliverable 12)

The Government will provide the contractor with the number of Government participants for the Kick-Off Meeting and the contractor shall provide sufficient copies of the presentation for all present.

The contractor shall draft and provide a Kick-Off Meeting Minutes Report (Section F, Deliverable 03) documenting the Kick-Off Meeting discussion and capturing any action items.

C.5.1.2 SUBTASK 2 – MONTHLY STATUS REPORT (MSR)

The contractor shall develop and provide an MSR (**Section J, Attachment D** (Section F, Deliverable 04). The MSR shall include the following:

a. Activities during reporting period, by task (include on-going activities, new activities, and activities completed, and progress to date on all above mentioned activities). Each section shall start with a brief description of the task.
b. Problems and corrective actions taken. Also include issues or concerns and proposed resolutions to address them.
c. Personnel gains, losses, and status (security clearance, etc.).
d. Government actions required.
e. Schedule (show major tasks, milestones, and deliverables; planned and actual start and completion dates for each).
f. Summary of Travel Planned for the next 30 days
g. Summary of trips taken, conferences attended, etc. (attach Trip Reports to the MSR for reporting period).
h. Accumulated invoiced cost for each CLIN up to the previous month.
i. Projected cost of each CLIN for the current month.

C.5.1.3 SUBTASK 3 – MONTHLY TECHNICAL STATUS MEETING

The contractor PM shall convene a monthly Technical Status Meeting with the TPOC, FEDSIM COR, and other Government stakeholders (Section F, Deliverable 05). The purpose of this meeting is to ensure all stakeholders are informed of the monthly activities and MSR, provide opportunities to identify other activities and establish priorities, and coordinate resolution of identified problems or opportunities. The contractor PM shall provide minutes of these meetings, including attendance, issues discussed, decisions made, and action items assigned, to the FEDSIM COR within five workdays following the meeting (Section F, Deliverable 06).

C.5.1.4 SUBTASK 4 – PROJECT MANAGEMENT PLAN (PMP)

The contractor shall document all support requirements in a PMP. The contractor shall provide the Government with a draft PMP (Section F, Deliverable 07) on which the Government will make comments. The final PMP (Section F, Deliverable 08) shall incorporate the Government's comments.

The PMP shall:

a. Describe the proposed management approach.
b. Contain Standard Operating Procedures (SOPs) for all tasks.
c. Include milestones, tasks, and subtasks required in this TO.

d. Provide for an overall Work Breakdown Structure (WBS) with a minimum of three levels and associated responsibilities and partnerships between Government organizations.
e. Describe in detail the contractor's approach to risk management under this TO.
f. Describe in detail the contractor's approach to communications, including processes, procedures, communication approach, and other rules of engagement between the contractor and the Government.
g. Include the contractor's Baseline QCP.

C.5.1.5 SUBTASK 5 – PREPARE TRIP REPORTS

The Government will identify the need for a Trip Report when the request for travel is submitted (Section F, Deliverable 10). The contractor shall keep a summary of all long-distance travel including, but not limited to, the name of the employee, location of travel, duration of trip, and Point of Contact (POC) at travel location. Trip reports shall also contain Government approval authority, total cost of the trip, a detailed description of the purpose of the trip, and any knowledge gained. At a minimum, trip reports shall be prepared with the information provided in **Section J, Attachment Q**.

C.5.1.6 SUBTASK 6 –QUALITY CONTROL PLAN (QCP)

The contractor shall develop a draft QCP (Section F, Deliverable 11), and deliver a final baselined QCP (Section F, Deliverable 12). The contractor shall periodically update the QCP, as required in Section F (Section F, Deliverable 13), as changes in program processes are identified.

Within the QCP, the contractor shall identify its approach for providing quality control in meeting the requirements of the TO. The contractor's QCP shall describe its quality control methodology for accomplishing TO performance expectations and objectives. The contractor shall fully discuss its validated processes and procedures that provide high quality performance for each Task Area. The QCP shall describe how the processes integrate with the Government's requirements.

C.5.1.7 SUBTASK 7 – FINANCIAL MANAGEMENT

The contractor shall provide financial reporting by cost element and include financial data. The contractor shall provide supplemental reporting including: resource planning; cost reporting; impacts assessments; invoicing; and disclosure requirements.

C.5.1.8 SUBTASK 8 – PRESENTATION MATERIALS

The contractor shall conduct presentations and participate in, or provide material for, meetings at times and places to be determined with the Government and contractor. Presentation material shall be due within five (5) days after the presentation (Section F, Deliverable 14).

C.5.1.9 SUBTASK 9 -TRANSITION-OUT

The contractor shall provide Transition-Out support when required by the Government. The Transition-Out Plan shall facilitate the accomplishment of a seamless transition from the incumbent to an incoming contractor/Government personnel at the expiration of the TO. The contractor shall provide a draft Transition-Out Plan within six months of Project Start (PS) (Section F, Deliverable 15). The Government will work with the contractor to finalize the

Transition-Out Plan (Section F, Deliverable 16) in accordance with Section F. At a minimum, this Transition-Out Plan shall be reviewed and updated NLT 90 calendar days prior to expiration of the TO (Section F, Deliverable 17).

In the Transition-Out Plan, the contractor shall identify how it will coordinate with the incoming contractor and/or Government personnel to transfer knowledge regarding the following:

a. Project management processes
b. Points of contact
c. Location of technical and project management documentation
d. Status of ongoing technical initiatives
e. Appropriate contractor to contractor coordination to ensure a seamless transition
f. Transition of Key Personnel
g. Schedules and milestones
h. Actions required of the Government

The contractor shall also establish and maintain effective communication with the incoming contractor/Government personnel for the period of the transition via weekly status meetings or as often as necessary to ensure a seamless Transition-Out.

The contractor shall implement its Transition-Out Plan NLT three months prior to expiration of the contract.

C.5.1.10 SUBTASK 10 – ACCOUNTING FOR CONTRACTOR MANPOWER REPORTING

The contractor shall report ALL contractor labor hours required for performance of services provided under this contract for the *US Army* via a secure data collection site. The contractor shall completely fill in all required data fields using the following web address: http://www.ecmra.mil/.

Reporting inputs will be for the labor executed during the period of performance during each Government Fiscal Year (FY), which runs October 1 through September 30. While inputs may be reported any time during the FY, all data shall be reported no later than October 31 of each calendar year. Contractors may direct questions to the support desk at: http://www.ecmra.mil/.

Contractors may use Extensible Markup Language (XML) data transfer to the database server or fill in the fields on the website. The XML direct transfer is a format for transferring files from a contractor's systems to the secure web site without the need for separate data entries for each required data element at the website. The specific formats for the XML direct transfer may be downloaded from the web.

C.5.2 TASK 2 – CYBER CAPABILITY DEVELOPMENT SUPPORT

The Contractor shall enhance INSCOM/RSC cyberspace capabilities that implement the cyberspace objectives of building technical capabilities for operations, to include a unified and integrated operational platform, accelerating research and development to provide DoD with a significant advantage in developing leap-ahead technologies to defend U.S. interests in cyberspace, and assessing Cyber Mission Force (CMF) capacity to achieve mission objectives when confronted with multiple contingencies. The Contractor shall develop rapid prototypes in

direct support to cyber operations performed by the operational users. The Contractor shall provide access and exploitation development, reverse engineering, vulnerability research, modeling & simulation, and application development for software, analytics, and systems under this subtask.

Specifically, in support of INSCOM/RSC, the Contractor shall provide support to include the following:

a. Develop tailored solutions and capabilities for cyber operations, cyber-support, and analytics for INCOM/RSC stakeholders;

b. Research and identify solutions with the potential of advancing cyberspace operations concepts and technologies and develop related analysis and recommendations;

c. Collaborate and confer with cyber operation capability developers and providers to understand supporting or related technologies and provide systems engineering-based recommendations;

d. Integrate cyber operations capabilities within system-of-systems concepts.

C.5.2.1 SUBTASK 1 – VULNERABILITY RESEARCH

The Contractor shall provide Vulnerability Research (VR) of INSCOM/RSC designated software and hardware systems. The systems will be provided as GFI at contract award and at appropriate program management milestones. This task requires the contractor to research systems to determine vulnerabilities in order to better enable user's (DoD and IC) freedom of operation within cyberspace. This research is designed to mitigate the adversary's attack vectors; to provide Intelligence, Surveillance, and Reconnaissance (ISR) employing analytics and related tools; and to provide improved continuous Situational Awareness (SA) of the cyber operations domain including modeling and simulation, assessments, and other supporting services. The contractor shall prepare and provide a Vulnerability Research Report (Section F, Deliverable 21) to reflect Vulnerability Research performed.

C.5.2.2 SUBTASK 2 – SECURITY RESEARCH

The Contractor shall provide security research of INSCOM, Army Cyber Command, Air Force Cyber Command, Navy Fleet Cyber Command, US Cyber Command, and National Security Agency designated software and hardware systems. The contractor shall:

a. Research and provide for the implementation of Information Assurance (IA) technologies and techniques to mitigate both external and internal threats

b. Research of innovative cryptographic models for authentication, authorization, and data security

c. Research of cyber operations attribution strategies; and research/data analytical models for non-repudiation.

The contractor shall prepare and provide a Security Research Report (Section F, Deliverable 22) to reflect security research performed.

C.5.2.3 SUBTASK 3 – MARKET RESEARCH

The Contractor shall perform and provide market research of cyber technologies to track and evaluate market trends and patterns. This includes the following scope of topics:

a. Broad scope cyberspace research and analysis;

b. Analysis of known cyber threats;

c. Research and assessment of new and emerging technologies within INSCOM/RSC designated research areas.

The contractor shall prepare and provide a Market Research Report (Section F, Deliverable 23) to reflect market research performed.

C.5.2.4 SUBTASK 4 – MALWARE ANALYSIS

The Contractor shall provide malware analysis, countermeasure assessment, and capability development support to include the following activities:

a. Identify new exploits and security vulnerabilities, analyze behavior of malicious code, research open source data, document host/network signatures, and develop mitigation and remediation strategies leveraging analytic models;

b. Compile data sets in order to perform dynamic and static analysis and reverse engineering of malware artifacts;

c. Develop, archive, and maintain findings in technical analysis and recommendation reports;

d. Support the release of analytics and technical reports by the Government;

e. Examine media and malware analysis reports and operational reporting from DoD incidents to correlate similar events, tradecraft, and TTPs of malicious activity. Develop, archive, and maintain analytics in support of operational assessments and reporting;

f. Conduct analysis on the lifecycle of adversary anatomy of attack and exploitation and the associated tools, malware, and encryption mechanisms utilized. Develop, archive, and maintain analytics in support of operational assessments and reporting.

The contractor shall prepare and provide a Malware Analysis Report (Section F, Deliverable 23) to reflect malware analysis, countermeasure assessment, and capability developments performed.

C.5.2.5 SUBTASK 5 – INFRASTRUCTURE DEVELOPMENT

The Contractor shall provide cyber infrastructure development and support. The contractor shall develop hardware infrastructure, virtualization infrastructure, and communications infrastructure in support of the INSCOM, Army Cyber Command, Air Force Cyber Command, Navy Fleet Cyber Command, US Cyber Command, and National Security Agency cyber operations objectives.

The contractor shall ensure that all development tasks will follow designated INSCOM/RSC processes for requirements review and analysis; design and development; verification; and test case. The contractor shall perform scenario development to ensure that the user's Concept of Operations (CONOPS) is fulfilled by the infrastructure.

The contractor shall provide design results, artifacts, and documentation generated throughout the development process capturing assessments for each mission stakeholders, resulting in an Infrastructure Development Plan. (Section F, Deliverable 19)

C.5.2.6 SUBTASK 6 – PLATFORM DEVELOPMENT

The Contractor shall provide platform development and support for INSCOM/RSC (Section F, Deliverable 29). The contractor shall further develop and sustain cyber Command and Control (C2) multiple complex, inter-related platforms (eg. ThunderRidge, Centurion) which interact with multiple communities; resource provisioning and monitoring platforms; operational planning tools and dashboards; and data processing, analysis, and visualization platforms for enabling ISR and Situational Awareness (SA) of the cyber area of operation.

The contractor shall ensure that all development tasks follow the INSCOM/RSC designated process for requirements review and analysis; design and development; verification; and test case and scenario development to ensure that the user's CONOPS is fulfilled by the platform. Results, artifacts, and documentation generated throughout the development process shall be provided as required.

C.5.2.7 SUBTASK 7 – CAPABILITY DEVELOPMENT

The Contractor shall provide cyber capability tool development (eg. ThunderRidge, Centurion) and support to ensure that technologies, services and other capabilities are both manageable and streamlined to their full extent (Section F, Deliverable 28). This task includes the development of full spectrum cyber capabilities to include software and hardware systems; sensors; data processing and analytic capabilities; cyber tools; and INSCOM/RSC designated emerging technologies and innovations. Development should consider full lifecycle supportability such as security, integration constraints based on the platform environment of the user.

The contractor shall ensure that all development tasks follow INSCOM/RSC designated processes for requirements review and analysis; design and development; verification; and testing. The contractor shall provide scenario development to ensure that the user's CONOPS is fulfilled by the capability. Results, artifacts, and documentation generated throughout the development process shall be provided as required.

C.5.2.8 SUBTASK 8 – INTEGRATION AND INTEROPERABILITY

The Contractor shall provide integration of developed cyber capabilities within the operational cyberspace environment, infrastructure, platforms, and capabilities.

This integration includes integration between INSCOM/RSC designated capabilities from the open source community, 3rd party Contractors, Other Government Agencies (OGA), and existing operational capabilities within the INSCOM environment.

The Contractor shall support interoperability testing and integration between developed cyber capabilities to enable joint cyber operations objectives. The integration technical diagram (Section F, Deliverable 27) should provide schematics and architectural artifacts documenting interfaces and data exchange entities.

C.5.2.9 SUBTASK 9 – TEST AND EVALUATION

The Contractor shall perform test and evaluation activities and provide analysis, recommendations, and reporting of these activities (Section F, Deliverable 25). Specifically, the contractor shall perform the following activities:

a. Provide automated test frameworks for the rapid verification of developed software; including exercised-based people, policy, and process assessments

b. Conduct T&E planning and preparation activities; including modeling and simulation tools and supporting analytics

c. Develop test plans, test cases, test procedures, and detailed results documents. Develop, archive, and maintain analytics in support of operational assessments and reporting

d. Conduct test and evaluation activities in accordance with Army and DoD testing and evaluation standards, collect and maintain results data, analyze data, and develop new processes and procedures to make existing test procedures more effective and relevant to mission requirements

e. Perform Developmental Testing (DT)

f. Perform Operational Testing (OT)

g. Perform Forensic Analysis and Characterization Testing (FACT);

h. Compile evidence data and reports in support of 3rd party Elevated Level of Assurance (ELA)

i. Conduct penetration testing of hardware and software systems and collect, maintain, and analyze collected data

j. Assess system security policies against client policies, identify system policies that are out of compliance with security requirements, provide recommendations and remediation of compliance failures

k. Conduct cyber capability vulnerability assessments customized to the system function and technical requirements to determine weaknesses and methods of exploitation that may result from improper system configuration, hardware or software flaws, or operational weaknesses.

C.5.3 TASK 3 – OPERATIONS AND MAINTENANCE INTEGRATION SUPPORT

The Contractor shall provide O&M support. This includes providing support for the integration of operational technologies (eg. ThunderRidge, Centurion), providing user training for operations and enhanced capabilities to include operational exercise support, providing system engineering and hardware/software/system administration, and providing support for Information Assurance best practices and formal accreditation processes.

C.5.3.1 SUBTASK 1 – OPERATIONAL SUPPORT

The Contractor shall provide operational support for developed cyber operations capabilities in support of the operational forces, to include Cyber Mission Force (CMF), National Mission Force (NMF), Cyber Protection Force (CPF), and Cyber Support teams. The contactor shall

provide both on-call as well as on-site personnel support for developed cyber operations capabilities.

The contractor shall provide support to all necessary preparation activities and after action activities performed to ensure continuity of knowledge and support throughout the lifecycle of the operational capabilities. Specific preparation support shall include integrated planning team support for the options of the activities:

a. Logistics and planning activities (people, material, supplies, etc)

b. Technical preparation

c. Objective preparation (rehearsal, dry run etc.).

Post-support activities shall include providing detailed After Action Reviews (AAR) (Section F, Deliverable 20) between technical staff, management, and the customer as well as any additional technical documentation and reports to ensure continuity of knowledge for future support activities and recommendations for optional courses of action.

The Contractor shall support the development, review and testing of Tactics, Technique, and Procedures (TTP) in support of cyber operations.

C.5.3.2 SUBTASK 2 – MAINTENANCE

The Contractor shall provide maintenance and refresh of cyber infrastructures, platforms, and capabilities (eg. ThunderRidge, Centurion) that have matured beyond the R&D phase. This task includes the continuous upkeep of the following items:

a. Source code repositories

b. Build artifacts

c. Executables

d. Data repositories

e. Test environments

f. Hardware infrastructure

The contractor shall provide knowledgeable development staff for maintenance support to ensure that the Contractor shall respond with rapid technical solutions for fielded products.

This subtask includes the troubleshooting and characterization of anomalies within the delivered products as well as the development and implementation of software patches. Maintenance support also includes the test, evaluation, and delivery of updates to capabilities.

The contractor shall provide support for and communication of feedback, lessons learned, and operational requests from the end users. All maintenance activities performed under this task shall be prioritized and executed with direction provided INSCOM/RSC.

C.5.3.3 SUBTASK 3 – TRAINING SUPPORT

The Contractor shall provide training to include cyber operations tool and technique training; on-demand operator training for requested capabilities; User Training (UT) for capabilities undergoing the formal testing process; train the trainer activities; interactive training tool and

module development; exercise preparation training; and integration training between capability stakeholders. All training support shall include the development and delivery of documentation, presentations, visualizations, and other training coursework. Where possible, training activities will leverage lessons learned and customer feedback to supplement the offering with content tailored to the end user or trainee (estimated at 30 users per quarter, via a mix of in-classroom and distance learning).

C.5.3.4 SUBTASK 4 – EXERCISE SUPPORT

The Contractor shall provide cyber exercise support and conduct assessments of technologies in collaboration and coordination with the INSCOM/RSC personnel, other support Contractors, end users, and other stakeholders (both internal and external).

The Contractor shall provide the following cyber exercise support:

a. Provide logistics, planning, and coordination support to the exercise;

b. Design and develop the exercise scenarios and mission objectives to test the efficiencies of the developed cyber capabilities, mission workflows, and organizational processes;

c. Support the site survey, site preparation, and hardware setup of the exercise environment;

d. Integrate infrastructures, platforms, and capabilities and ensure interoperability with exercise partners and their connected systems for conducting the exercise;

e. Provide on-site personnel support and Subject Matter Expertise (SME) for the execution of the exercise objectives;

f. Provide white team, red team, and blue team services as required by the exercise

g. Develop and maintain exercise analytics and data to prepare, update, and deliver feedback reports describing findings, assessments, impacts, recommended scenario modifications, and lessons learned.

The contractor shall prepare and provide an Exercise Feedback Report (Section F, Deliverable 26) to reflect findings, assessments, impacts, recommended scenario modifications, and lessons learned for each exercise.

C.5.3.5 SUBTASK 5 – SYSTEMS ENGINEERING AND ADMINISTRATION SUPPORT

The Contractor shall provide hardware infrastructure, virtualization, data repositories, networking, embedded system, and software application administration support in accordance with mission requirements.

Specifically, the contractor shall provide support to the following activities:

a. Operate, maintain, identify, and manage risks to Government information systems to include new technical information systems solutions (both physical and virtual)

b. Develop, maintain, and refresh [cloud-based] proprietary information systems and obtain appropriate Government approval prior to implementing new technical information systems solutions (both physical and virtual)

c. Maintain operating systems and refer/coordinate/interact with the appropriate Government employees or other Contractors to maintain applications

d. Develop, maintain, and refresh network drawings and document configuration information

e. Apply and document system updates, patches and configuration changes

f. Respond to exercise, crisis, or contingency situations by providing system support and systems administration of Government IT assets both hardware and software

g. Configure, troubleshoot, and maintain hardware devices required to maintain an operational and secure infrastructure

h. Configure, upgrade, troubleshoot, diagnose, test, monitor, and document operating systems, COTS/GOTS software applications and other various procured software

i. Repair and/or resolve hardware issues, which may require travel to and from remote buildings

j. Coordinate the repair of hardware devices covered by OEM warranties to include performing initial diagnostics, contacting/escorting Contractors, and arranging for receipt and return of equipment

k. Document the work completed in accordance with existing technical writing and system documentation requirements